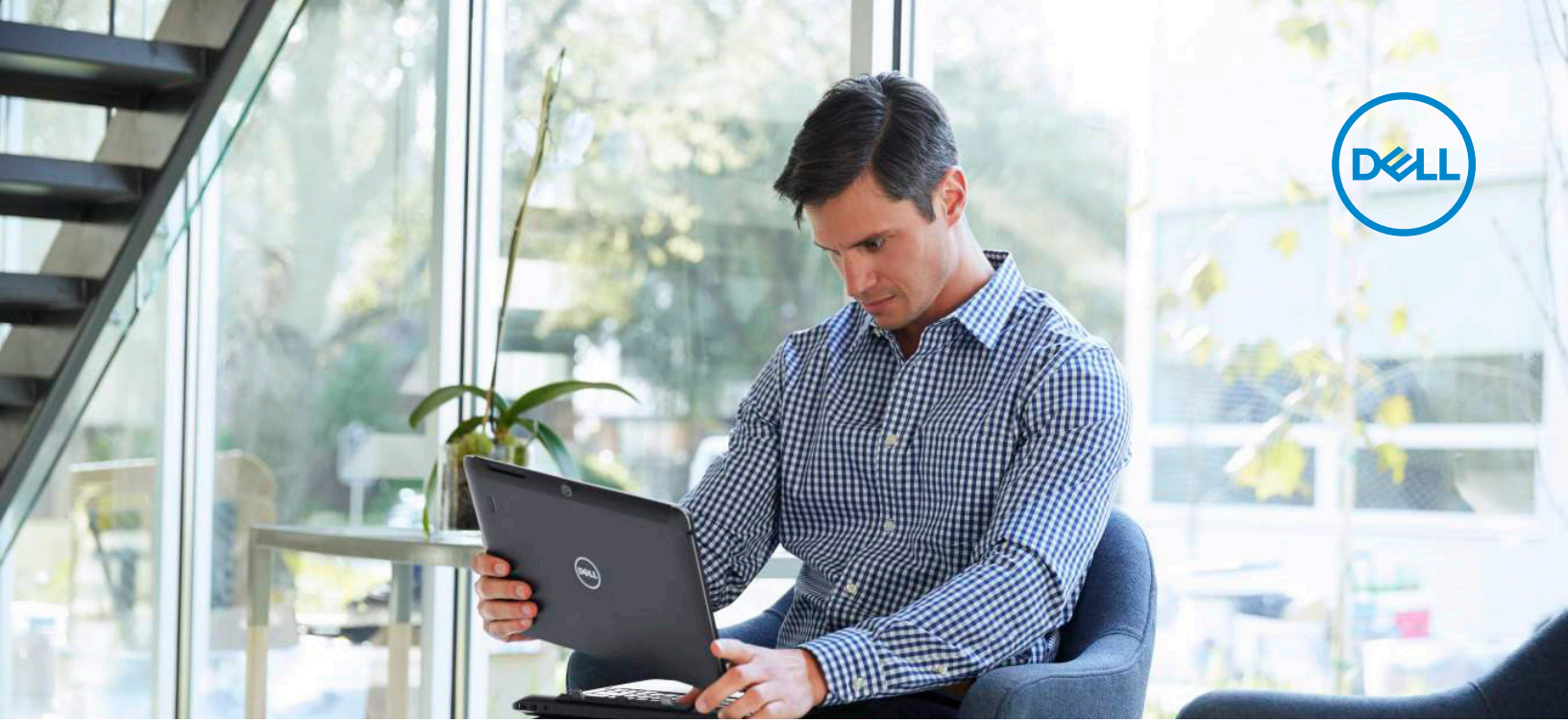

## Advanced Threat Prevention Benefits

- Unparalleled efficacy, stops 99% of malware before it can even run, far above the average 50% efficacy rating of the top anti-virus solutions[1]
- Preventing malware significantly reduces remediation costs and end user down time
- Protects physical PCs, virtual desktops and servers
- Low CPU and memory usage enhances system performance to give you back the computer you thought you bought
- Local detection with no need for a constant cloud connection ensures mobile end users can work without fear of compromise
- Prevention based on AI and Mathematical models with minimal false positives increases IT productivity and eliminates the need for constant signature updates
- Satisfies PCI DSS, HIPAA HITECH and Microsoft requirements for an anti-virus replacement to reduce your overall data protection cost

[1]Results from Cylance Unbelievable Demo Tour, Austin, Houston and Dallas Texas, May 2015

# Dell Endpoint Security Suite Enterprise

### Stop evolving attacks, simplify endpoint security and exceed compliance

Endpoint security and compliance are critical to every organization, no matter the size. Organizations must secure physical and virtual endpoint devices and the data on them, while still satisfying end user requirements to embrace computing trends like bring-your-own-device (BYOD), sharing data in public cloud services and workforce mobility. Traditional data security point solutions attempt to address these needs, but managing multiple clients and consoles is difficult for resource constrained IT teams, especially those without security experts in house. Most endpoint protection solutions are difficult to deploy and manage, lack coverage for all the places employees put and use data and reduce system performance and end user productivity. Dell's data security suite offers a number of advantages, including:

- Sales and support for your physical PCs, virtual desktops and security solutions from one source
- Protection for heterogeneous environments with full support for Dell and non-Dell hardware, as well as virtual desktops running on Citrix or VMware
- Automatic deployment and provisioning when factory-installed on Dell commercial devices
- Single integrated client simplifies deployment and updates and ensures all elements of your data security solution work seamlessly together
- Easy compliance and auditing with pre-defined reports and an intuitive management console that quickly guides you to any issues that need to be addressed

Endpoint Security Suite Enterprise offers strong data security for business data, systems and reputations. The suite offers an integrated client that includes advanced threat prevention, Enterprise class encryption, all centrally-managed via a single console to help businesses reduce IT management costs and complexity. With consolidated compliance reporting and flexible email notifications, businesses can easily enforce and prove compliance for all of their endpoints. Built in security with features like simplified policy configuration with smart defaults and pre-defined report templates are especially helpful as organizations struggle to protect end users and data

## Advanced Threat Prevention

The constantly evolving threat landscape requires a level of security that far exceeds the effectiveness of current solutions deployed throughout enterprises, government and institutions worldwide. Traditional, behavior- or signature-based anti-virus and anti-malware solutions are reactive by design since they depend on previously seen behaviors or patterns to identify an attack. Because of this reactive design they are increasingly ineffective against Zero-Day threats, advanced persistent threats and targeted attacks like Spear Phishing and Ransomware.

Endpoint Security Suite Enterprise solves this problem by integrating revolutionary advanced threat prevention with unparalleled efficacy against zero-day threats, advanced persistent threats and commodity malware. This solution uses unique artificial intelligence (AI) and dynamic mathematical models to analyze files prior to their execution and determine which are safe and which aren't, thus stopping malware before it can even run. Based on tens of thousands of markers extracted from careful analyses of millions of real-world exploits and known good files, the Dell approach does not rely on signatures that look for known behaviors or patterns and that must be updated as threats evolve. This allows us to prevent threats without the need for a constant cloud connection or frequent updates. The intelligence is built into the endpoint, whether it is a physical device or a virtual machine. Dell rounds out this advanced threat prevention by checking Dell commercial system BIOS on boot, to quickly alert administrators of any possible BIOS tampering.

## Web protection and host-based firewall

With rapidly growing attack surface, organizations require defense in depth. Protecting users against multiple attack vectors is critical to endpoint security. In addition to the predictive mathematical model that stops vast majority of threats from running, the suite offers additional protection from web borne attacks as well as a host-based firewall for additional device level protection against malware that slip past the perimeter firewall. The web protection functionality offers a reputation based website rating. With web reputation rating available for over 106 million URL's it covers 95% of popular trafficked web sites. The host-based firewall functionality offers superior protection vs native Windows firewall and is feature rich and application aware. This helps control inbound and outbound traffic based on rules as well as optional global threat intelligence reputation scoring. Meets the requirements of the Children's Internet Protection Act, (CIPA).

## AirGap

Today more than ever before many businesses, especially critical infrastructures such as federal government entities, oil rigs, utility providers and financial services need to be ultra secure to protect against a determined bunch of malicious actors. With Endpoint Security Suite Enterprise these entities can now deploy the industry's first endpoint suite that combines data-centric encyption and advanced threat prevention in a completely disconnected mode from the cloud. With very little cloud dependency to stop emerging threats, the enterprise suite is a great fit for these organizations that are concerned with determined attackers sneaking in a new malware. While traditional AV solutions mostly likely will not catch these threats without constant updates which is difficult and burdensome on IT in air gapped networks, the enterprise suite can effectively catch a vast majority of these while requiring far fewer updates and no cloud connection.

## Encryption

Dell Encryption is a flexible suite of enhanced security solutions that enables data protection whether located on physical PCs or virtual desktops–without disrupting IT processes or end user productivity. Our Encryption solution offered as a part of the Enterprise Suite license, enables flexible choices from multiple encryption technologies including Data Centric encryption, Software Full Disk Encryption, enhanced centralized management of native encryption (Microsoft BitLocker and Mac FireVault) and protection of data on external media, self-encrypting drives, PC's and Servers. Designed for easy deployment, end-user transparency and hassle-free compliance, Dell Encryption delivers a high level of protection, fills critical security gaps and allows you to manage encryption policies for multiple endpoints and operating systems - all from a single management console. It allows the administrator to easily enforce encryption policies wherever the data resides without end user intervention. Our encryption offers many benefits including:

- Flexibility to choose from multiple encryption solutions including File and Folder Encryption, Software Full Disk Encryption, management of native encryption across multiple operating systems.
- Detailed, enterprise-wide encryption status reporting to avoid costly fines and damaged reputations if a device is lost or stolen
- No special disk preparation or defragmenting required before encryption
- Integration with existing processes for authentication, automated patch management and more
- Encryption of all data, except files essential to booting the operating system or full disk encryption, depending on your preference
- Enhanced port control system to prevent data leakage

## Technical Specifications

Endpoint Security Suite Enterprise is available for mixed vendor environments that meet the below specifications.

**Supported Client Operating Systems**:

- Microsoft Windows 7 Ultimate, Enterprise and Professional Editions
- Microsoft Windows 8 and 8.1 Enterprise and Professional Editions
- Microsoft Windows 10 Education, Enterprise and Pro Editions
- Microsoft Windows Server 2008 R2, 2012 R2 and 2016
- Windows Embedded Standard Thin Client OS - WES7 32 and 64 bit support (ATP only)
- macOS 10.9+, 10.10+, 10.11+ & 10.12+
- Linux - RHEL Cent-OS (ATP only)

**Supported VDI environments on Dell select PowerEdge VDI servers**:

- Windows 10 virtual desktops

**Running on the following hypervisors and connection brokers**:

- VMware vSphere 6.0 update 2 and VMware Horizon 7
- Microsoft Hyper-V 2012 R2 and Citrix XenDesktop 7.11

**Remote management console and Compliance Reporter access are supported via the following Internet Browsers**:

- Internet Explorer 11.x or later
- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later

**Supports IPv6**

## Services

We offer an end-to-end portfolio of services to plan, implement and maintain your security solutions. Our team of security experts will help you asses and identify areas of improvement, implement and optimize solutions efficiently and provide peace of mind with 24/7 comprehensive technical support. Contact your Dell Data Security Specialist for more details.

**Learn more at Dell.com/DataSecurity and Dell.com/wyse/shield**